CLAIMS

What is claimed is:

5   1.   A method for authorizing a command from a user in a network device

including:

    establishing a RADIUS session with the user;

    receiving a user profile for the user from an Authentication, Authorization,

and Accounting (AAA) server, said user profile containing information regarding

10 which commands the user is authorized to execute;

    storing said user profile in a memory;

    receiving the command from the user;

    determining whether the command is authorized based on said information

in said user profile stored in said memory; and

15   authorizing or rejecting the command based on the results of said

determining.

    2.   The method of claim 1, wherein the network device is a Network Access

Server (NAS).

20

    3.   The method of claim 1, further including purging said user profile from

said memory when said RADIUS session is terminated.

4.   The method of claim 1, wherein said determining includes comparing said

command to a command set contained in said user profile and said authorizing

includes authorizing the command if it is contained in said command set.

5

5.   The method of claim 4, wherein said command set is a list of previously

authorized commands.

6.   The method of claim 4, wherein said command set is described by regular

10   expressions.

7.   An apparatus for authorizing a command from a user in a network device

including:

a RADIUS session initiator;

15   a user profile receiver coupled to said RADIUS session initiator;

a memory;

a user profile storer coupled to said user profile receiver and said memory;

a command receiver;

an authorized command determiner coupled to said command receiver and

20   to said memory; and

a command authorizer coupled to said authorized command determiner.

8.   The apparatus of claim 7, wherein the network device is a Network Access Server (NAS).

9.   The apparatus of claim 7, further including a user profile purger coupled to

5   said memory.

10.   The apparatus of claim 7, wherein said authorized command determiner includes a command set comparer coupled to said memory and wherein said memory includes a user profile having a command set.

10

11.   The apparatus of claim 10, wherein said command set is a list of previously authorized commands.

12.   The apparatus of claim 10, wherein said command set is described by

15   regular expressions.

13.   An apparatus for authorizing a command from a user in a network device including:

       means for establishing a RADIUS session with the user;

20   means for receiving a user profile for the user from an Authentication, Authorization, and Accounting (AAA) server, said user profile containing information regarding which commands the user is authorized to execute;

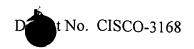means for storing said user profile in a memory;

means for receiving the command from the user;

means for determining whether the command is authorized based on said

information in said user profile stored in said memory; and

5   means for authorizing or rejecting the command based on the results of said

determining.

14.   The apparatus of claim 13, wherein the network device is a Network Access

Server (NAS).

10

15.   The apparatus of claim 13, further including means for purging said user

profile from said memory when said RADIUS session is terminated.

16.   The apparatus of claim 13, wherein said means for determining includes

15   means for comparing said command to a command set contained in said user

profile and said means for authorizing includes means for authorizing the

command if it is contained in said command set.

17.   The apparatus of claim 16, wherein said command set is a list of authorized

20   commands.

18.   The apparatus of claim 16, wherein said command set is described by

regular expressions.

19.   A program storage device readable by a machine, tangibly embodying a

5   program of instructions executable by the machine to perform a method for

authorizing a command from a user in a network device, the method including:

establishing a RADIUS session with the user;

receiving a user profile for the user from an Authentication, Authorization,

and Accounting (AAA) server, said user profile containing information regarding

10   which commands the user is authorized to execute;

storing said user profile in a memory;

receiving the command from the user;

determining whether the command is authorized based on said information

in said user profile stored in said memory; and

15   authorizing or rejecting the command based on the results of said

determining.